

貢献度に応じた公平な連合学習の実現に向けて

— 異質なデータ価値の下での 補助金付きデータ共有メカニズムの設計 —

増田 真之介*

*京都大学大学院情報学研究科

1 研究背景と目的

データは機械学習モデルの汎化性能を向上させるうえで中心的な役割を果たすが、単一の組織が収集できるデータの量とその多様性には、しばしば限界がある。このことから、複数のエージェントにデータ提供を促すためのデータ提供メカニズムが重要となる。Karimireddy et al. [2022] は、モデル精度を報酬として、データをより多く共有したエージェントにより良いモデルを配布する Accuracy Shaping(AS)を提案した。Bornstein et al. [2024] は金銭的報酬をASと組み合わせることで、さらなるデータ提供を促すメカニズムへ拡張した。

一方、実際のデータ共有では、データ源によって希少性や品質、対象タスクに対する有用性が異なる。したがって、単純なデータ量ではなく、各データ源の価値を考慮してデータ提供を促す必要がある。本研究では、各エージェントのデータ価値を考慮した補助金設計を行い、限られた予算のもとで得られる総有効データ量を最大化することを目的とする。

2 問題の定式化

n 人のデータ提供者を考え、エージェント i はデータ提供量 $m_i \geq 0$ を選択する。エージェント i のデータ源に対応する有効データ関数を $h_i: [0, \infty) \rightarrow [0, \infty)$ とし、 h_i は連続、狭義単調増加かつ凹であり、 $h_i(0) = 0$ と仮定する。ここで、 $h_i(m_i)$ はデータ源ごとの対象タスクへの関連性や希少性、アノテーション品質、データの冗長性などを反映した有効データ量を表し、 h_i の凹性は同一のデータ源から追加的にデータを収集する際の限界的な有効データ価値

の通減を表す。データの単位収集コストを $c_i > 0$ とする。各エージェントはモデルの予測性能と金銭的報酬から効用を得るものとする。有効データ量 $h_i(m_i)$ から達成可能なモデル精度を $a(h_i(m_i)) = \max\{0, a_{\text{opt}} - \frac{k}{h_i(m_i)}\}$ とする。ここで、 a_{opt} は達成可能な最大精度、 $k > 0$ は学習タスクの難易度を表すパラメータである。この精度関数は、有効データ量の増加に伴ってモデル精度が向上する一方、その改善幅が通減することを表している。また、 $\max\{0, \cdot\}$ は、データ量が少なくモデルが実用可能な性能に達しない領域では、モデル精度から得られる効用をゼロとすることを表す。

中央計画者は有限の予算 B を用いて、総有効データ量を最大化するようなメカニズムを設計することが目的である。メカニズムは各エージェントの拠出データ量に応じた、モデル精度と金銭的報酬を返すメカニズムを設計する際には、各エージェントが参加によって単独で学習する場合以上の効用を得られることに加え (IR)、エージェントに返却するモデル精度が全提供データから達成可能な精度を超えないこと (FC) が必要である。AS は、図 1 に示されるように、各エージェントの個人最適値 m_i^* を超えるデータ提供を促すため、返却するモデル精度を線形に増加させ (Shaping Line)、その領域で限界効用が正となるように設計する。AS に従うエージェントの最適反応は、この Shaping Line と返却できるモデル精度の上限である Feasibility Curve との交点 m_i^* となる。本研究では IR と FC を満たしつつ、図 2 のように、AS の構造に対してエージェント固有の補助金 r_i を加えて、Shaping Line の傾きを変化させることで最適反応の位置 m_i^* を調整し、Nash 均衡における総有効データ量を最大化する Subsidized Accuracy Shaping

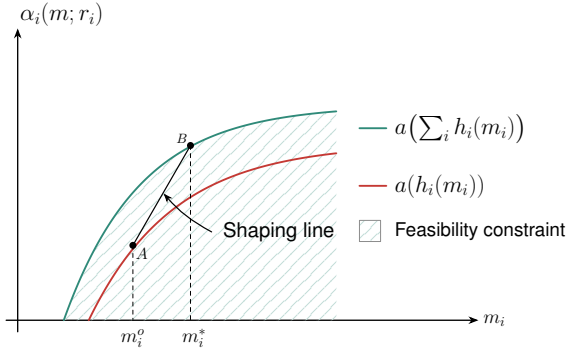


図 1: Accuracy Shaping

(SubAS) を考える. 具体的なメカニズムの定義は以下の式で表される. m_i が $m_i \leq m_i^0$ の時, メカニズムは $a(h_i(m_i))$, $R_i = 0$ を返却する. $m_i^0 < m_i < m_i^*$ においては,

$$\alpha_i = a(h_i(m_i^0)) + (c_i - r_i + \epsilon)(m_i - m_i^0),$$

$$R_i = r_i(m_i - m_i^0)$$

とする. 一方, $m_i \geq m_i^*$ では,

$$\alpha_i = a\left(\sum_{j=1}^n h_j(m_j)\right), \quad R_i = r_i(m_i^* - m_i^0)$$

ここで, m_i^* は Shaping Line と Feasibility Curve との交点で表され, Nash 均衡を求めるには, 全エージェントの最適反応条件を同時に満たす必要がある.

3 研究成果

中央計画者は, 各エージェントへの補助金 r_i を決定し, 限られた予算 B のもとで, Nash 均衡における総有効データ量を最大化することを目的とする. すなわち,

$$\begin{aligned} & \text{maximize}_{0 \leq r_i < c_i + \epsilon} \sum_{i=1}^n h_i(m_i^*(\mathbf{r})) \\ & \text{subject to} \quad \sum_{i=1}^n r_i(m_i^*(\mathbf{r}) - m_i^0) \leq B, \end{aligned} \quad (1)$$

という最適化問題を考える. ここで, 中央計画者が補助金 $\mathbf{r}$ を選択し, その補助金に応じて各エージェント

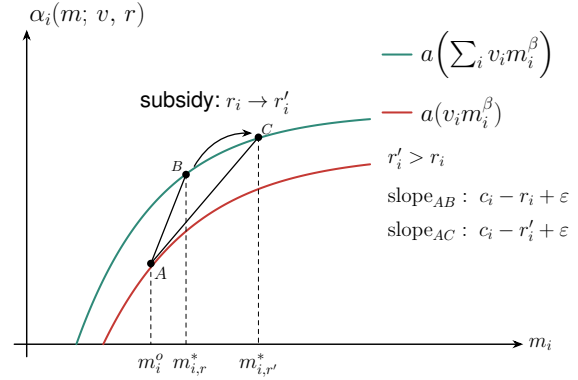


図 2: Subsidized Accuracy Shaping

がデータ提供量を決定するため, (1) は中央計画者を leader, エージェントを followers とする Stackelberg 型の二段階最適化問題である.

前節で述べたように, 各エージェントの最適反応は Shaping Line と Feasibility Curve の交点である m_i^* として一意に定まる. しかし, この交点は他のエージェントのデータ提供量にも依存するため, Nash 均衡を直接計算するには複数の最適反応を同時に求める必要がある. そこで, 総有効データ量

$$Z = \sum_{i=1}^n h_i(m_i) \quad (2)$$

を導入する. 交点条件を整理すると, 各エージェントの均衡時の提供量を Z の関数として表すことができるため, Nash 均衡条件全体を

$$Z = \Psi_{\mathbf{r}}(Z) \quad (3)$$

という 1 次元の自己整合方程式に縮約できる. さらに, 各 h_i の凹性を利用することで, 有効な領域においてこの自己整合方程式の解が一意となり, Nash 均衡も一意に決定される.

一方, (1) では補助金 $\mathbf{r}$ を変更するたびに Nash 均衡 $\mathbf{m}^*(\mathbf{r})$ も変化するため, 当初は複雑な非線形最適化問題として数値的に解く必要があると考えていた. しかし, 目標とする総有効データ量 Z をあらかじめ固定し, その Z を実現するために必要な補助金を最小化する問題へ変換することで, 問題の構造を単純化できることが分かった.

具体的には, Shaping Line と Feasibility Curve の交点条件を用いて補助金 r_i を消去すると, 固定した

Z に対する補助金支出は各 m_i の線形関数として表すことができる．また，目標とする総有効データ量を達成する条件は

$$\sum_{i=1}^n h_i(m_i) \geq Z \quad (4)$$

となる．元の等式制約は，達成可能な Z の範囲では，目的関数が各 m_i に対して単調増加であるため，不等式に緩和しても最適点では等号が成立する．また，各 h_i は凹関数であるため，左辺は凹関数であり，この制約が定める領域は凸集合となる．したがって，当初は複雑な非線形最適化と考えていた補助金設計問題を，固定した Z に対する凸最適化問題へ変換できることが分かった．

以上より，元の多次元な Stackelberg 型最適化問題を直接解く代わりに，まず Nash 均衡を総有効データ量 Z に関する 1 次元の自己整合方程式へ縮約し，さらに各 Z に対する補助金設計を凸最適化として解くことができる．最終的には， Z を 1 次元的に探索しながら必要な最小補助金を計算することで，予算 B のもとで達成可能な最大の総有効データ量を求められる．

4 今後の課題

今後の課題としては， h_i の形状の違いによる補助金配分の変化， h_i や c_i の推定にノイズがある場合の均衡に与える影響の解析などが挙げられる．また，本研究では先行研究に従いデータ共有を仮定したモデルを扱ったが，今後は，各クライアントがローカルデータを保持したままモデル更新情報を共有する，実際の連合学習の設定への拡張を検討する．

参考文献

- Marco Bornstein, Amrit Singh Bedi, Anit Kumar Sahu, Furqan Khan, and Furong Huang. Towards realistic mechanisms that incentivize federated participation and contribution, 2024. URL <https://arxiv.org/abs/2310.13681>.
- Sai Praneeth Karimireddy, Wenshuo Guo, and Michael I. Jordan. Mechanisms that incentivize data sharing in federated learning, 2022. URL <https://arxiv.org/abs/2207.04557>.